APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/919,240	07/31/2001	Daryl Carvis Cromer	RPS9 2000 0079	2810

7590   01/13/2005

IBM Corporation
Personal Systems Group Legal Dept.
Dept. 9CCA/Bldg. 002-2
P.O. Box 12195
Research Triangle Park, NC 27709

EXAMINER
PYZOCHA, MICHAEL J

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondenc address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 July 2001*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date *07312001*.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-25 are pending.

Claim Rejections - 35 USC § 112

2.   The following is a quotation of the second paragraph of 35
U.S.C. 112:

> The specification shall conclude with one or more claims particularly
> pointing out and distinctly claiming the subject matter which the applicant
> regards as his invention.

3.   Claims 13-18 are rejected under 35 U.S.C. 112, second

paragraph, as being indefinite for failing to particularly point

out and distinctly claim the subject matter which applicant

regards as the invention.

4.   Claim 13 recites the limitation "said removable computer

readable medium" in line 4.   There is insufficient antecedent

basis for this limitation in the claim. The word "removable"

will be ignored for the purposes of applying prior art.

5.   Any claim not specifically addressed is rejected by virtue

of its dependencies.

Claim Rejections - 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which

forms the basis for all obviousness rejections set forth in this

Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7.   Claims 1-7, 11-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sibert (U.S. 6,832,316)`, further in view of Tello (U.S. 6,463,537)`, and further in view of Langford (U.S. 6,507,911).

As per claim 1, Sibert discloses a method providing security for a plurality of data records stored on a computer-readable medium within a computing system, wherein said computer readable medium additionally stores a first data structure, starting at a first location within said computer readable medium, locating data records in said plurality thereof, said method a decryption subroutine executed as said computing system is being initialized, said decryption subroutine includes determining that electrical power has been turned on in said computing system, reading said encrypted version of said first data structure from said nonvolatile storage, decrypting said encrypted version of said first data structure to form said first data structure (see column 6 lines 55-67) and a method for encrypting (see column 5 lines 41-67).

Sibert fails to disclose the encryption subroutine includes receiving a request to shut down said computing system, reading said first data structure from said computer readable medium, encrypting said first data structure to produce an encrypted version of said first data structure.

However, Tello teaches performing tasks at shut down (see column 14 lines 1-41).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to perform Sibert's method of encryption at shut down as taught by Tello.

Motivation to do so would have been to hide data storage devices (see Tello column 14 lines 1-41).

The modified Sibert and Tello system fails to disclose, as a part of the encryption method, deleting said first data structure from said computer readable medium, and storing said encrypted version of said first data structure in nonvolatile storage, starting at a second location within said nonvolatile storage, and, as a part of the decryption method, writing said data structure to said computer readable medium, starting at said first location.

However, Langford teaches such a replacement method (see column 4 line 63 through column 5 line 18).

At the time of the invention it would have been obvious to
a person of ordinary skill in the art to use Langford's method
of overwriting in the modified Sibert and Tello system.

Motivation to do so would have been to allow no plaintext
of the original data to be present (see Langford column 5 lines
1-18).

As per claims 2-3, the modified Sibert, Tello and Langford
system discloses the second location is at the first location on
the readable medium (see Langford column 4 line 63 through
column 5 line 18).

As per claim 4, the modified Sibert, Tello and Langford
system discloses the nonvolatile storage is a memory structure,
separate from said computer readable medium, with said computing
system (see Sibert column 6 lines 55-67).

As per claim 5, the modified Sibert, Tello and Langford
system discloses encryption of said first data structure occurs
within a cryptographic processor in said computing system using
an encryption key, said cryptographic processor is separate from
a system processor within said computing system, and decryption
of said encrypted version of said first data structure occurs
within said cryptographic processor in said computing system
using a decryption key generated from data stored in secure
storage accessed by said cryptographic processor (see Sibert

column 5 lines 49-56 and column 6 lines 61-67 where the "cryptographic circuitry" is the processor).

As per claim 6, the modified Sibert, Tello and Langford system discloses a public key of said computing system is used for encryption of said first data structure, and a private key of said computing system is used for decryption of said encrypted version of said first data structure (see Tello column 8 lines 34-40).

As per claim 7, the modified Sibert, Tello and Langford system discloses the encrypted version of said first data structure is equal in length to said first data structure (see Langford column 4 line 62 through column 5 line 18).

As per claims 11-12, the modified Sibert, Tello and Langford system discloses said method additionally comprises a configuration subroutine providing a user interface for setting and resetting a configuration bit, and said encryption subroutine is executed according to a state of said configuration bit and said encryption subroutine additionally includes setting a flag bit in non-volatile storage, and said decryption subroutine is executed only when said flag bit is set (see Tello column 14 lines 34-40 where it is inherent that a bit is set for encryption and decryption should only happen for encrypted data).

As per claims 13 and 19, the modified Sibert, Tello and

Langford system discloses a method providing security for a

plurality of data records stored on a computer readable medium

within a computing system, wherein said computer medium

additionally stores a first data structure starting at a first

location within said removable computer readable medium,

locating data records in said plurality thereof, said method

comprises an encryption subroutine executed to encrypt said

first data structure and a decryption subroutine subsequently

executed to decrypt an encrypted version of said first data

structure, said encryption subroutine includes reading said

first data structure from said computer readable medium,

encrypting said first data structure within a cryptographic

processor in said computing system using an encryption key to

produce an encrypted version of said first data structure,

deleting said first data structure from said computer readable

medium, and storing said encrypted version of said first data

structure in nonvolatile storage, starting at a second location

within said nonvolatile storage, and said decryption subroutine

includes reading said encrypted version of said first data

structure from said nonvolatile storage, decrypting said

encrypted version of said first data structure within said

cryptographic processor in said computing system using a

decryption key generated from data stored in secure storage

accessed by said cryptographic processor to form said first data

structure, and writing said data structure to said computer

readable medium, starting at said first location (see rejection

of claim 5).

Claims 14-16 and 20-22 are rejected as in claims 1, 11-12

respectively.

As per claims 17-18 and 23-24, the modified Sibert, Tello

and Langford system discloses a cryptographic selection

subroutine providing a graphical user interlace, said

cryptographic selection subroutine includes displaying a choice

between encryption and decryption, displaying representations of

computer readable medium in said computing system, and receiving

a cryptographic selection signal indicative of whether

encryption or decryption is to occur and of a chosen computer

readable medium, said encryption subroutine is executed in

response to receiving cryptographic selection signal indicating

encryption is to occur, with said first data structure of said

chosen computer readable medium being encrypted, and said

decryption subroutine is executed in response to receiving a

cryptographic selection signal indicating decryption is to

occur, and with said encrypted version of said first data

structure of said chosen computer readable medium being

decrypted wherein said encrypted version of said first data

structure is stored in nonvolatile storage on said chosen

computer readable medium (see Langford column 6 lines 52-67 for

the GUI and the encryption/decryption and hard drives as in

Tello and Sibert applied to previous claims).

8.   Claims 8-9 and 25 are rejected under 35 U.S.C. 103(a) as

being unpatentable over the modified Sibert, Tello and Langford

system as applied to claims 1 and 19 above, and further in view

of Robinson et al (U.S. 5,544,356).

    As per claims 8-9 and 25, the modified Sibert, Tello and

Langford system fails to disclose the computer readable medium

additionally stores a second data structure, starting at a

second location within said computer readable medium, describing

characteristics of said first data structure, and said

encryption subroutine additionally includes reading said second

data structure to determine characteristics of said first data

structure wherein said first data structure is a file allocation

table, and said second data structure is a boot record.

    However, Robinson et al teaches a boot record describing

the file allocation table (see column 1 line 64 through column 2

line 4).

    At the time of the invention it would have been obvious to

a person of ordinary skill in the art to use the modified

Sibert, Tello and Langford system to encrypt Robinson et al's

file allocation table.

Motivation to do so would have been that the boot record

includes the number of copies of the file allocation table (see

Robinson et al column 1 line 64 through column 2 line 4).

9.   Claims 8, 10 and 25 are rejected under 35 U.S.C. 103(a) as

being unpatentable over the modified Sibert, Tello and Langford

system as applied to claims 1 and 19 above, and further in view

of Starek et al (U.S. 6,070,174).

As per claims 8, 10 and 25, the modified Sibert, Tello and

Langford system fails to disclose the computer readable medium

additionally stores a second data structure, starting at a

second location within said computer readable medium, describing

characteristics of said first data structure, and said

encryption subroutine additionally includes reading said second

data structure to determine characteristics of said first data

structure wherein said first data structure includes an array of

file records in a master file table of a NTFS file, and said

second data structure includes metafile data in said master file

table.

However, Starek et al teaches such data structures (see

column 10 lines 29-51).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the modified Sibert, Tello and Langford system to encrypt Starek et al's file array.

Motivation to do so would have been that the metafile describe the file system structure (see column 10 lines 29-51).

10.   Claims 1-25 are rejected as above but in view of JP2001202167A, which discloses a control method for a computer, involves encrypting and decoding data on memory based on power supply ON/OFF.

Conclusion

11.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Rollins (US 20020141588 A1) discloses a method for data security for digital data, Flyntz (US 6351817 B1) discloses encrypting the data on a hard drive at the end of a user session, Sherman et al (US 6249868 B1) discloses a method for securing data on a hard drive, Kong (US 5884026 A) discloses a method for protecting an operating system, Pereira (US 5809230 A) discloses encrypting

and rewriting a MBR to a disk, Cummins (US 5007082 A) discloses

a data security method using an encryption/decryption algorithm

which attaches at the primitive BIOS level of the operating

system, and Allen et al (US 4757533 A) discloses a method for

hard disc protection.

Any inquiry concerning this communication or earlier

communications from the examiner should be directed to Michael

Pyzocha whose telephone number is (571) 272-3875. The examiner

can normally be reached on 7:00am - 4:30pm first Fridays of the

bi-week off.

If attempts to reach the examiner by telephone are

unsuccessful, the examiner's supervisor, Andrew Caldwell can be

reached on (571) 272-3868. The fax phone number for the

organization where this application or proceeding is assigned is

703-872-9306.

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER